

Amendments to the Claims

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Currently amended) A method for detecting a fraud event in a distributed telecommunications network, wherein the distributed network enables performance of at least two functions selected from a non exhaustive list comprising: an access function, a transport function, an application function, a management function and a security function, by respective functional groups of elements, at least two of the functional groups having respectively different characteristics, and wherein each of the groups comprising comprises at least one element capable of performing operations related to at least the function of said particular functional group and operative to create records on said operations,

the method comprising steps of:

obtaining records data related to at least one telecommunications session and originating from at least two

of the elements each belonging to at least a respective one of
the at least two said functional groups,

analyzing the records data thus obtained to determine whether
there is a lack of consistency between the records data
respectively obtained from said at least two functional groups
and relating to the same at least one telecommunications
session, and

if the lack of consistency is determined, concluding that
there is a fraud event.

2. (Original) The method according to Claim 1, wherein said
distributed telecommunications network is packet-based.

3. (Currently amended) The method according to Claim 1,
wherein the functions are in different network layers, and the
step of obtaining the records data is characterized in
that each of said at least two elements from which the records
data originates are associated with functions in respectively
different network layers belongs to a different functional
group.

4. (Original) The method according to Claim 1, wherein said
records data originating from a particular element comprises

at least a portion of original records or a derivative of the original records.

5. (Original) The method according to Claim 4, wherein the derivative of the original records are statistically processed original records.

6. (Original) The method according to Claim 1, wherein the step of analyzing comprises a sub-step of recognizing and forming, from the obtained records data, corresponding data respectively associated with said at least two functional groups.

7. (Original) The method according to Claim 6, comprising using, for recognizing the corresponding data, at least one identifier field and/or at least one value field, wherein said at least one identifier field is selected from a non-exhausting list comprising data fields for identifying source, destination, IP address, user name, phone number, and said at least one value field is selected from a non-exhausting list comprising data fields for indicating values of login time, connect time, time of first packet of a flow, logout time, disconnect time, time of last packet of a flow,

incoming byte count, outgoing byte count, duration, packet count, session count, dollar value, quality of service .

8. (Original) The method according to Claim 7, wherein the step of analyzing comprises a sub-step of applying fraud detection rules for determining whether there is a lack of consistency between the corresponding data respectively obtained from said at least two functional groups.

9. (Original) The method according to Claim 8, wherein the fraud detection rules comprise a collection of algorithms for detection various types of fraud and specifying: selection of elements from which the records data is to be obtained, combinations of identifier fields and/or value fields to be used for recognizing the corresponding data, combinations of the identifier fields and/or value fields to be further checked and/or compared in the corresponding data and methods of comparing thereof, errors and/or trigger thresholds to be referred to when making a decision concerning presence of a fraud event.

10. (Original) The method according to Claim 9, wherein the method comprises a preliminary step of selecting two or more

particular elements belonging to different functional groups to obtain the records data from each of said two or more selected elements; and upon obtaining said records data, performing sub-steps of the analyzing step:

- determining, in the records data obtained from each of said elements, presence or absence of an expected specified identifier field, and
- considering the lack of consistency to take place if said specified expected identifier field is present in the records data obtained from at least one of said two or more elements, while being absent in the records data obtained from at least one of said two or more elements.

11. (Original) The method according to Claim 9, wherein the method comprises a preliminary step of selecting two or more particular elements belonging to different functional groups to obtain the records data from each of said two or more selected elements; and upon obtaining said records data, performing sub-steps of the analyzing step:

- determining, in the records data obtained from each of said two or more elements, presence or absence of a specified value field, and

- considering the lack of consistency to take place either if said specified value field is absent in the records data obtained from at least one of said two or more elements, while present in the records data obtained from at least one of them, or if values of the specified value fields respectively associated with said two or more elements do not correspond to one another.

12. (Previously presented) The method according to Claim 9, wherein the method comprises a preliminary step of selecting two or more particular elements belonging to different functional groups to obtain the records data from each of said two or more selected elements; and upon obtaining said records data, performing sub-steps of the analyzing step:

-determining, in the records data obtained from each of said at least two functional groups, presence of at least one specified identifier field and at least one specified value field; and

-considering the lack of consistency to take place if said at least one specified identifier field and/or said at least one specified value field associated with one of said two or more elements do not respectively correspond to that or those associated with another one of said at least two functional groups.

13. (Currently amended) An apparatus for detecting a fraud event in a distributed telecommunications network comprising
at least two or more different functional groups of elements,
at least two of the functional groups having respectively
different characteristics, the apparatus comprising
an analyzer unit capable of analyzing records data related to
at least one telecommunications session and originating from
at least two elements each belonging to a respective one of
said at least two or more different functional groups, to
determine whether there is a lack of consistency between the
records data parts respectively associated with said at least
two different functional groups and relating to the same at
least one telecommunications session, and capable of
indicating the fraud event whenever the lack of consistency is
determined.

14. (Original) The apparatus according to Claim 13, further comprising an interface unit for collecting the records data related to at least one telecommunications session and originating from one or more elements belonging to said two or more different functional groups.

15. (Original) The apparatus according to Claim 13, adapted to cooperate with the distributed network enabling performance of at least two functions selected from a list comprising: an access function, a transport function, an application function, a management function and a security function, by respective said functional groups of the elements and wherein each of the groups comprising at least one element capable of performing operations related to at least the function of said particular functional group and operative to create records on said operations.

16. (Original) The apparatus according to Claim 14, further comprising a pre-processor unit for preparing the records data collected from said interface unit for said analyzer unit.

17. (Original) The apparatus according to Claim 13, further comprising one or more units selected from a non-exhausting

list comprising an actions unit, an operator panel unit and a rule builder unit configured to store and develop rules for detecting a fraud event.

18. (Currently amended) A system for detecting a fraud event in a distributed telecommunications network, wherein the distributed network enables performance of at least two functions selected from a list comprising: an access function, a transport function, an application function, a management function and a security function by different respective functional groups of elements, at least two of the different functional groups having respectively different characteristics, ; the system comprising — and the at least two different said functional groups each comprising at least one element capable of performing operations related to at least the function of said particular functional group and operative to create records on said operations, said system comprising:
- a fraud detection apparatus capable of analyzing records data related to at least one telecommunications session and originating from at least two of the elements each belonging to a respective one of said at least two different functional groups to determine whether

there is a lack of consistency between the records data parts respectively obtained from said at least two different functional groups and wherein the records data parts relate to the same at least one telecommunications session, and concluding that there is a fraud event if the lack of consistency is determined.

19. (Currently amended) A program storage device readable by a machine, tangibly embodying a program of instructions executable by the machine to perform method steps, for detecting a fraud event in a distributed telecommunications network, wherein said steps being:
analyzing records data related to at least one telecommunications session and originating from at least two elements each belonging to a respective one of at least two different functional groups having respectively different characteristics to determine whether there is a lack of consistency between the records data parts respectively associated with said at least two functional groups and wherein the records data parts relate to the same at least one telecommunications session, and if the lack of consistency is determined, concluding that there is a fraud event.

20. (Currently amended) A computer program product comprising a computer useable medium having computer readable program code embodied therein for detecting a fraud event in a distributed telecommunications network, the computer program product comprising:

a computer readable program code for causing the computer to analyze records data related to at least one telecommunications session and originating from at least two elements each belonging to a respective one of at least two different functional groups having respectively different characteristics, to determine whether there is a lack of consistency between the records data parts respectively associated with said at least two different functional groups and wherein the records data parts relate to the same at least one telecommunications session, and a computer readable program code for causing the computer, if the lack of consistency is determined, to conclude that there is a fraud event.